Alibaba Cloud
操作审计

Tutorials

Issue: 20200401

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. **You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.**
2. **No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.**
3. **The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.**
4. **This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequent**

ial, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Document conventions

Style	Description	Example
	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 **Danger:** Resetting will result in the loss of user configuration data.
	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 **Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 **Notice:** If the weight is set to 0, the server no longer receives new requests.
	A note indicates supplemental instructions, best practices, tips, and other content.	 **Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click Settings > Network > Set network type.
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands.	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *`Instance_ID`*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`

Style	Description	Example
{} or {a|b}	**This format is used for a required value, where only one item can be selected.**	`switch {active|stand}`

Contents

1 Authorize RAM users to use ActionTrail

This topic describes how to create custom policies to grant permissions to RAM users so that they can log on to the ActionTrail console and use the corresponding ActionTrail resources.

Prerequisites

- **An Alibaba Cloud account is created. If not,** *create an Alibaba Cloud account* **first.**
- **View the supported ActionTrail API operations and RAM permission policies. For more information, see** *#unique_4*.

Procedure

1. *#unique_5*.
2. *#unique_6*.

   You can create custom policies to grant permissions to RAM users based on the following *examples of permission policies*.
3. *#unique_7*.

Examples of permission policies

- **Example 1: Grant read-only permissions to a RAM user.**

```
{
    "Version": "1",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "actiontrail:LookupEvents",
            "actiontrail:Describe*",
            "actiontrail:Get*"
        ],
        "Resource": "*"
    }]
}
```

- **Example 2: Grant read-only permissions to a RAM user when the RAM user logs on from a specified IP address.**

```
{
    "Version": "1",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "actiontrail:LookupEvents",
            "actiontrail:Describe*",
```

```
            "actiontrail:Get*"
        ],
        "Resource": "*",
        "Condition":{
            "IpAddress": {
                "acs:SourceIp": "42.120.XX.X/24"
            }
        }
    }]
}
```

2 Use ActionTrail to monitor the use of your AccessKey ID

This topic describes how to use ActionTrail to deliver events to Log Service and monitor the use of your AccessKey ID or configure an alert in Log Service.

Prerequisites

An Alibaba Cloud account is created. If not, *create an Alibaba Cloud account* first.

Context

After activating ActionTrail, you can query events recorded in the last 90 days. You can query events based on your AccessKey ID. For more information, see *#unique_9*. You can also deliver events to Log Service to store the event logs for a longer period of time.

Create a trail

1. **Log on to the *ActionTrail console*.**
2. **In the top navigation bar, select the region where you want to create a trail.**

   Note:
   The region that you select becomes the home region of the trail to be created.
3. **In the left-side navigation pane, choose ActionTrail > Trails.**
4. **Click Create Trail. On the page that appears, enter a name in the Trail Name field.**
5. **Set Apply Trail to All Regions to Yes.**
6. **Set Event Type to All.**
7. **Turn on the Enable Logging switch and set Deliver Events To to SLS Logstore.**
8. **Set Create Log Service Project to Yes, select a region from the Log Service Region drop-down list, and then enter a project name in the Log Service Project field.**

   Note:
   The Log Service project specified here is used to store event logs delivered by ActionTrail. You can enter the name of an existing project in the selected region or enter a new project name.
9. **Click Confirm.**

10. In the dialog box that appears, click Activate.

> **Note:**
> To create a trail, you need to authorize ActionTrail to access Log Service and Object Storage Service (OSS). If you have granted the permissions, this dialog box does not appear.

11. On the page that appears, click Activate Log Service.

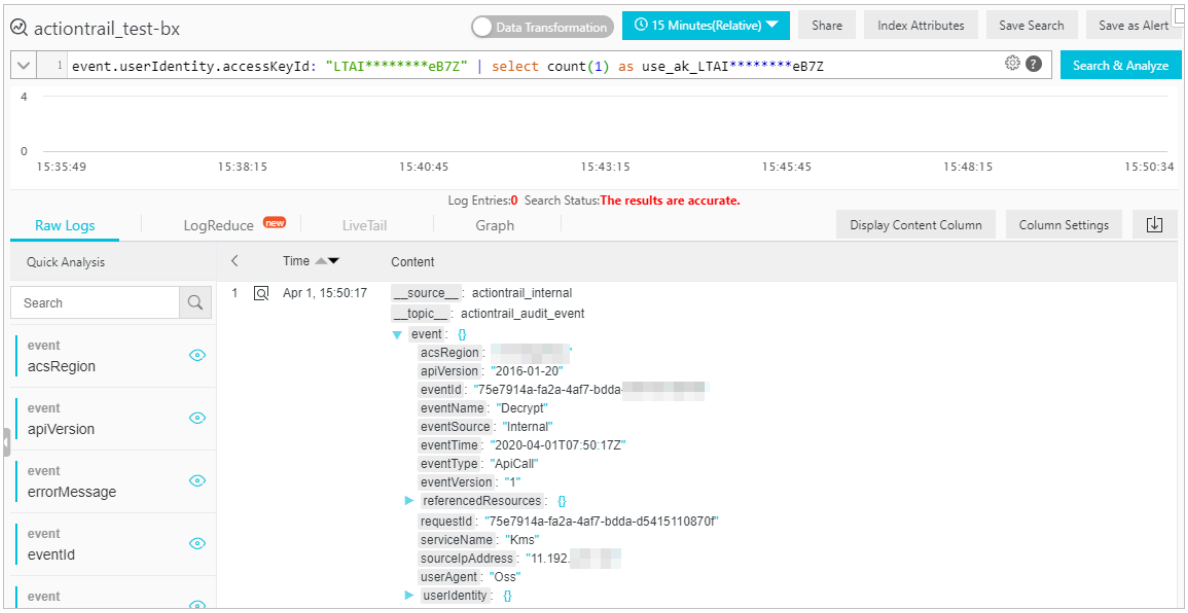
> **Note:**
> After you create the trail, ActionTrail delivers events in all regions to a Logstore in the specified Log Service project.

Configure Log Service

1. On the Trails page, find the target trail and click Log analysis in the Log Service Links column.

> **Note:**
> You can also log on to the *Log Service console* to configure the service.

2. Enter `event.userIdentity.accessKeyId: "LTAI********eB7Z" | select count(1) as use_ak_LTAI********eB7Z` in the search bar and click Search & Analyze.



3. **Save the search or configure an alert based on the search.**
   - **Save the search: Click Save Search in the upper-right corner. In the dialog box that appears, set Saved Search Name and click OK.**

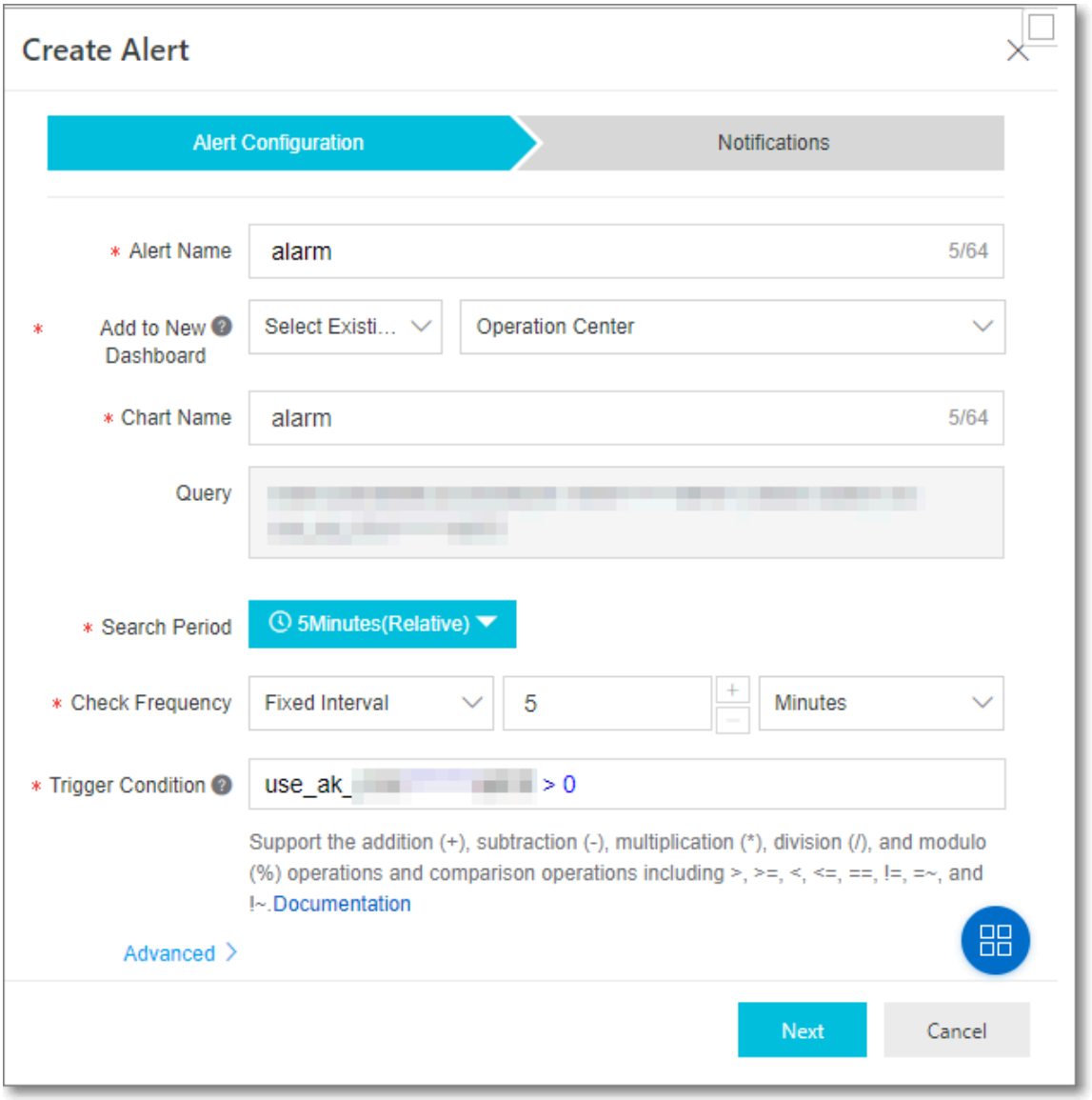
     Note:

After you save the search, you can select it in the Log Service console to quickly initiate the search.

For more information about a saved search, see *#unique_10*.

- **Configure an alert based on the search: Click Saved as Alert in the upper-right corner. In the Alert Configuration step, set the alert parameters, as shown in the following figure. In the Notifications step, select a notification method.**

  For more information about how to configure an alert, see *#unique_11*.



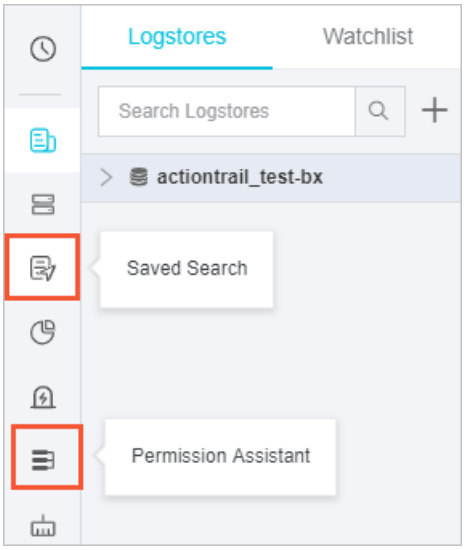
Note:

After you configure the alert, you will receive an alert notification when the alert is triggered. For example, according to the alert configuration shown in the preceding figure, Log Service checks the use of your AccessKey ID at an

interval of five minutes. If your AccessKey ID is used, Log Service generates an alert.

Result

You can view and manage the saved search and alerts in the Log Service console.



3 Use ActionTrail to monitor the use of your Alibaba Cloud account

This topic describes how to use ActionTrail to deliver events to Log Service and monitor the use of your Alibaba Cloud account or configure an alert in Log Service.

Prerequisites

An Alibaba Cloud account is created. If not, *create an Alibaba Cloud account* first.

Create a trail

1. **Log on to the *ActionTrail console*.**
2. **In the top navigation bar, select the region where you want to create a trail.**

   Note:
   The region that you select becomes the home region of the trail to be created.
3. **In the left-side navigation pane, choose ActionTrail > Trails.**
4. **Click Create Trail. On the page that appears, enter a name in the Trail Name field.**
5. **Set Apply Trail to All Regions to Yes.**
6. **Set Event Type to All.**
7. **Turn on the Enable Logging switch and set Deliver Events To to SLS Logstore.**
8. **Set Create Log Service Project to Yes, select a region from the Log Service Region drop-down list, and then enter a project name in the Log Service Project field.**

   Note:
   The Log Service project specified here is used to store event logs delivered by ActionTrail. You can enter the name of an existing project in the selected region or enter a new project name.
9. **Click Confirm.**
10. **In the dialog box that appears, click Activate.**

    Note:

To create a trail, you need to authorize ActionTrail to access Log Service and Object Storage Service (OSS). If you have granted the permissions, this dialog box does not appear.

11. **On the page that appears, click Activate Log Service.**

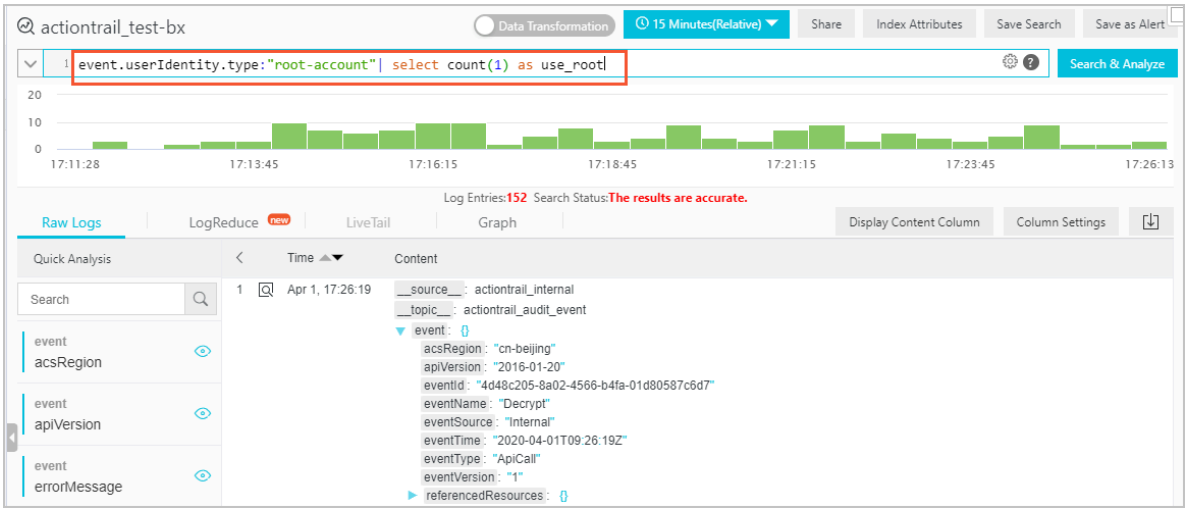
> **Note:**
> **After you create the trail, ActionTrail delivers events in all regions to a Logstore in the specified Log Service project.**

Configure Log Service

1. **On the Trails page, find the target trail and click Log analysis in the Log Service Links column.**

> **Note:**
> **You can also log on to the *Log Service console* to configure the service.**

2. **Enter `event.userIdentity.type:"root-account"| select count(1) as use_root` in the search bar and click Search & Analyze.**



3. **Save the search or configure an alert based on the search.**

   - **Save the search: Click Save Search in the upper-right corner. In the dialog box that appears, set Saved Search Name and click OK.**

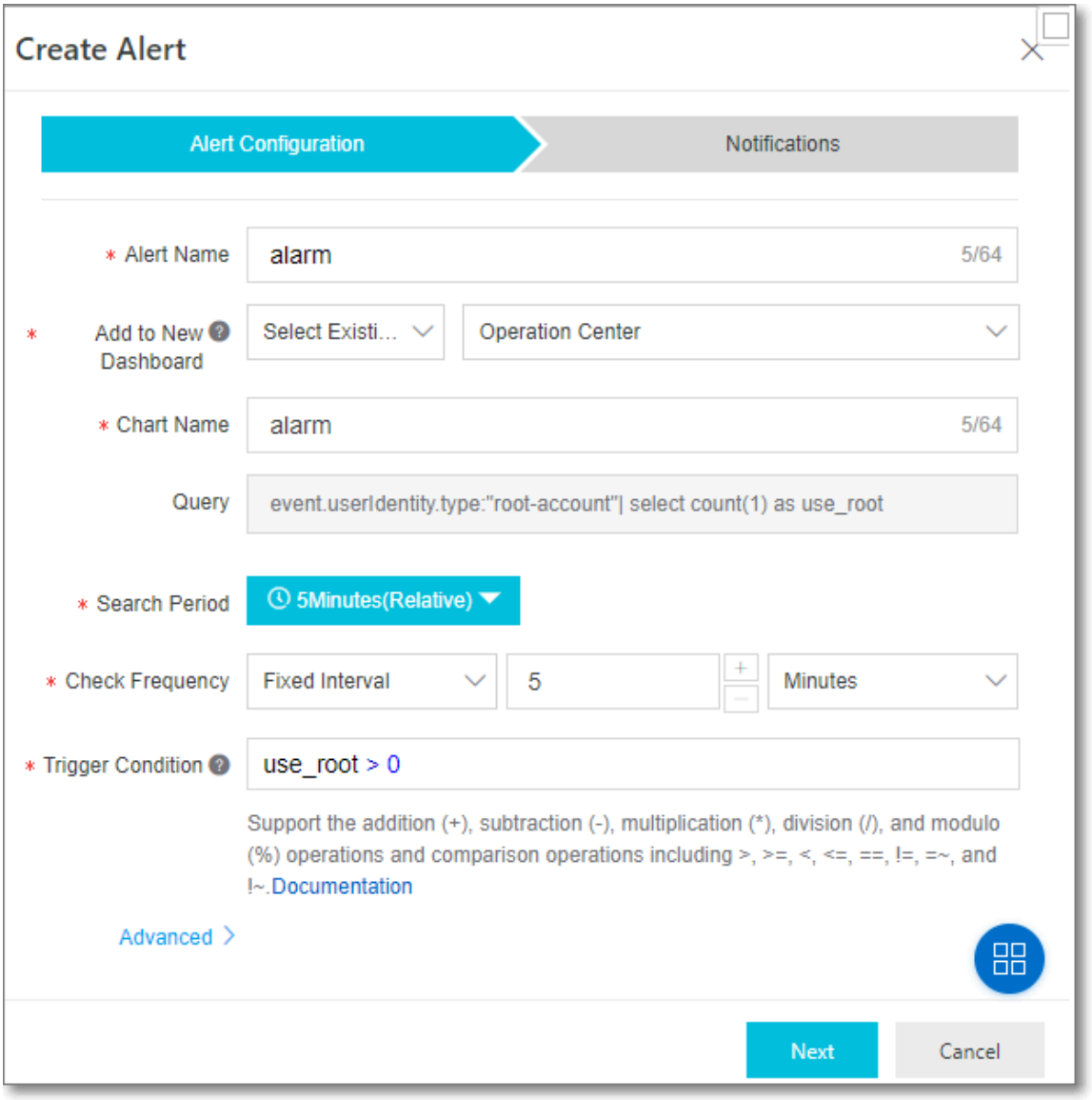
> **Note:**

After you save the search, you can select it in the Log Service console to quickly initiate the search.

For more information about a saved search, see *#unique_10*.

- **Configure an alert based on the search: Click Saved as Alert in the upper-right corner. In the Alert Configuration step, set the alert parameters, as shown in the following figure. In the Notifications step, select a notification method.**

  For more information about how to configure an alert, see *#unique_11*.



Note:

After you configure the alert, you will receive an alert notification when the alert is triggered. For example, according to the alert configuration shown in the preceding figure, Log Service checks the use of your Alibaba Cloud

account at an interval of five minutes. If your Alibaba Cloud account is used, Log Service generates an alert.

Result

You can view and manage the saved search and alerts in the Log Service console.